I CLAIM

sub a1

1. A computer system comprising a first node, a second node and a communications link connecting the first node and the second node, and wherein initially the system is capable of working in a plurality of modes, including a first mode corresponding to in-clear working over the link, a second mode corresponding to encrypted working over the link, and a third mode employed for migration from in-clear to encrypted working over the link, and wherein the third mode provides in-clear working until means required for encrypted working are provided at both the first and the second nodes, when encrypted working is commenced and from which point in time only encrypted working is possible over the link.

2. A computer system comprising a first node, a second node and a communications link connecting the first node and the second node, wherein the system is initially capable of operating in a plurality of modes, including a first mode corresponding to in-clear working over the link, a second mode corresponding to encrypted working over the link, and a third mode, employed for migration from in-clear working over the link to encrypted working over the link, in which one said node is set to "initiate encryption" and the other said node is set to "accept encryption", and wherein the third mode provides in-clear working until means required for encrypted working are installed at both the first and the second nodes, when encrypted working is provided over the link and from which point in time only encrypted working is possible over the link.

3. A computer system as claimed in claim 2, wherein the means required for encrypted working comprise a long term key, which long term key is used to establish a message encryption key to be employed by the first and the second nodes for encryption and decryption of messages transmitted over the link.

4. A computer system as claimed in claim 3, wherein the first and second nodes each include a respective cache, in both of which caches a said message encryption key is stored upon its establishment.

5. A computer system as claimed in claim 4, wherein when there is a failure to establish a said message encryption key a special key value is cached in the cache of a said node set to "initiate encryption", the presence of which special key value serves to suspend attempts to establish a said message encryption key.

6. A computer system as claimed in claim 2 and wherein each said node includes policy files for controlling setting to one of the three modes of operation.

7. A computer system capable of operation as a virtual private network (VPN) including at least one central server and at least one remote client connectable by a shared network, wherein the or each server and the or each client include respective security policy files with settings of "in-clear", "initiate encryption" or "accept encryption", and "encrypt" for information to be transmitted therebetween, "in-clear" corresponding to a mode of operation comprising working in-clear, "encrypt" corresponding to a mode of operation comprising encrypted VPN working over the network, and "initiate encryption" or "accept encryption", being employed for a mode of operation when migration from in-clear to encrypted VPN working is required, which migration mode provides in-clear working until authentication keys required for encrypted working are installed at both ends of a particular server/client link across the network, when encrypted VPN working is provided for said link and from which point in time only encrypted working is possible over said link.

8. A computer system as claimed in claim 7 and further including means serving to reset the security policy files at both ends of the link to "encrypt" from "initiate encryption" or "accept encryption", in response to receipt of a message indicating installation of the authentication keys at both ends of said link.

9. A method for use in migrating operation of a computer system from in-clear working to encrypted working, the computer system comprising a first node, a second node and a communications link connecting the first and second nodes, the computer system initially being capable of operating in a plurality of modes including "in-clear" mode, migration mode having settings of "initiate encryption" or "accept encryption", and "encrypt" mode,

means enabling encrypted working being required to be installed at the first and second nodes before encrypted working can commence, the method including the steps of installing said means at the first node, setting the first node to "initiate encryption", setting the second node to "accept encryption", as a result of which messages transmitted between said nodes are transmitted in-clear, subsequently installing said means at the second node, as a result of which messages between the nodes are transmitted encrypted, and setting the first and second nodes to "encrypt" mode whereby only encrypted working is subsequently possible over the link.

10. A method for use in migrating operation of a computer system, comprising at least one central server and at least one remote client connectable by a shared network, from in-clear working to virtual private network (VPN) working, including the step of providing the or each server and the or each client with respective security policy files having settings for "in-clear", "initiate encryption" or "accept encryption", and "encrypt" for information to be transmitted therebetween, "in-clear" corresponding to a mode of operation comprising working in-clear, "encrypt" corresponding to a mode of operation comprising encrypted VPN working over the network, and "initiate encryption" or "accept encryption" corresponding to a mode of operation which is employed when migration from in-clear to encrypted VPN working is required and which provides in-clear working until authentication keys required for encrypted working are installed, and including the steps of setting the policy file on the server of a particular link to "initiate encryption" and setting the policy file on the client of said particular link to "accept encryption" when migration is required, installing the authentication key at the server of said particular link, messages between the server and the client of the particular link thereby being transmitted in clear, subsequently installing the authentication keys at the client of said particular link whereby encrypted VPN working commences instead of in-clear working, and resetting the security policy files of the server and client of said particular link to "encrypt" whereby only encrypted working is subsequently possible over said link.